de Rechtspraak

Raad voor de
rechtspraak

De minister van Veiligheid en Justitie
mr. I.W. Opstelten
Postbus 20301
2500 EH Den Haag

Directie Strategie en
Ontwikkeling

bezoekadres
Kneuterdijk 1
2514 EM Den Haag

correspondentieadres
Postbus 90613
2509 LP Den Haag

T (088) 36 10000
F (088) 36 10022
www.rechtspraak.nl

datum	4 juli 2013
contactpersoon	
doorkiesnummer	
e-mail	
ons kenmerk	
uw kenmerk	
onderwerp	Advies Wetsvoorstel computercriminaliteit III
bijlage(n)	1

Geachte heer Opstelten,

Bij brief van 2 mei jl. met opgemeld kenmerk verzocht u de Raad voor de rechtspraak (de "**Raad**") u te adviseren inzake het Wetsvoorstel Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) (het "**Wetsvoorstel**") en de bijbehorende Memorie van Toelichting ("**MvT**").

Het Wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken, en vormt een uitwerking van eerdere toezeggingen aan de Tweede Kamer en van het in het regeerakkoord van dit kabinet opgenomen voornemen om de toenemende bedreigingen en kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden door het juridisch instrumentarium aan te passen naar aanleiding van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie.

Het Wetsvoorstel bevat – naast enkele technische wetswijzigingen – de volgende elementen:

1. Het creëren van een nieuwe bevoegdheid voor bepaalde opsporingsambtenaren om een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk te kunnen binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Daarbij kan de beveiliging worden doorbroken of kunnen technische handelingen worden verricht om toegang te verschaffen tot het geautomatiseerde werk. Ook kan heimelijk software worden geïnstalleerd met behulp waarvan op specifieke punten de beveiliging wordt doorbroken of omzeild en waarmee de versleuteling van gegevens ongedaan kan worden gemaakt. (*Onderzoek in een geautomatiseerd werk*).[1]

[1] Art. 125ja Sv (nieuw).

2. Het aanpassen van de regeling van de bevoegdheid van de officier van justitie om, met machtiging van de rechter-commissaris, te bevelen dat gegevens op internet ontoegankelijk worden gemaakt. (*Bevel tot ontoegankelijk maken van gegevens).*[2]
3. Het creëren van een afzonderlijke wettelijke bevoegdheid tot het geven van een bevel aan een verdachte tot het verschaffen van toegang tot versleutelde elektronische gegevens en het toegankelijk maken van die gegevens. (*Decryptiebevel*).[3]
4. Het strafbaar stellen van het wederrechtelijk overnemen van gegevens en het voorhanden hebben of bekend maken van door misdrijf verkregen gegevens. Daardoor worden gedragingen strafbaar die kunnen worden beschouwd als "heling" van computergegevens. (*Strafbaarstelling heling van gegevens).*[4]

Gehoord de gerechten, adviseert de Raad als volgt.[5]

Advies

Algemeen: Inbreuk op persoonlijke levenssfeer vergt voorafgaande rechterlijke toetsing
De inzet van de voorgestelde opsporingsbevoegdheden (de hiervoor beschreven elementen 1-3) kan een vergaande inbreuk op grondrechten van burgers (verdachten of derden) opleveren, zoals het recht op de eerbiediging van de persoonlijke levenssfeer en het brief-, telefoon- en telegraafgeheim. Zoals ook in de MvT tot uiting komt, is het van groot belang dat een dergelijke inbreuk zo beperkt mogelijk wordt gehouden en dat de burger wordt beschermd tegen willekeurige inmenging door de overheid in zijn privéleven. Het Wetsvoorstel bepaalt in dit verband dat deze bevoegdheden slechts kunnen worden toegepast na een schriftelijke machtiging door de rechter-commissaris. Daarnaast wordt in de MvT meermalen het belang van de toetsing door de rechter-commissaris op – naast rechtmatigheid – de beginselen van proportionaliteit en subsidiariteit benadrukt. De Raad acht de keuze voor een dergelijke voorafgaande rechterlijke toetsing ten aanzien van de voorgestelde opsporingsbevoegdheden wenselijk en verstandig.[6]

---

[2] Art 125p Sv (nieuw).
[3] Art. 125k Sv (nieuw).
[4] Art. 138c Sr en 139f Sr (nieuw).
[5] De Raad voor de rechtspraak heeft op grond van artikel 95 van de Wet op de rechterlijke organisatie een wettelijke adviestaak met betrekking tot nieuwe wets- en beleidsvoorstellen die gevolgen hebben voor de rechtspraak. De adviezen worden vastgesteld na overleg met de gerechten. De Raad voor de rechtspraak is een adviescollege in de zin van artikel 79 en 80 van de Grondwet. Bij het opstellen van zijn adviezen beoordeelt de Raad de voorgenomen wet- en regelgeving in het bijzonder op de gevolgen voor de organisatie en de werklast van de gerechten en op de (praktische) toepasbaarheid en uitvoerbaarheid. Rechters zijn bij de behandeling van individuele zaken niet gebonden aan de inhoud van de wetgevingsadviezen van de Raad voor de rechtspraak.
[6] Zie in dit verband ook de opmerkingen van de Raad in zijn advies over een eerder ontwerp van dit voorstel in het licht van EHRM 14 september 2010, Sanoma Uitgevers B.V. tegen Nederland (Advies van 30 september 2010, gepubliceerd op www.rechtspraak.nl onder nummer 2010/38, met name p. 3). Zie voorts de opmerkingen van de Raad over de noodzaak van betrokkenheid van de rechter-commissaris bij ingrijpende maatregelen in het voorbereidend onderzoek in zijn advies over het wetsontwerp conservatoir beslag ten behoeve van slachtoffers (advies nr. 2011/43), en de voorgestelde aanpassing van art. 97 Sv in het wetsontwerp bronbescherming voor journalisten, waarover de Raad in 2011 adviseerde (advies nr. 2011/15).

Onderzoek in een geautomatiseerd werk
Het Wetsvoorstel omvat als gezegd onder meer een nieuwe bevoegdheid voor bepaalde opsporingsambtenaren om een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen. Het moet dan wel gaan om een verdenking van een feit waarvoor voorlopige hechtenis mogelijk is. Bovendien kan het binnendringen enkel plaatsvinden met een vooraf gespecificeerd doel. In de MvT wordt uitvoerig ingegaan op de noodzaak van de invoering van deze nieuwe bevoegdheid. Gesteld wordt dat de bestaande opsporingsbevoegdheden in toenemende mate tekort schieten om aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit tegemoet te komen. De gebleken knelpunten zijn de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken en het gebruik van *cloudcomputing*-diensten. In de MvT wordt voorts uiteengezet waarom niet met de huidige bevoegdheden kan worden volstaan.

De Raad herkent de in de MvT genoemde knelpunten en problemen voor de opsporingspraktijk. De vraag naar mogelijkheden om direct toegang te krijgen tot een geautomatiseerd werk, dus bijvoorbeeld zonder inmenging van eventuele *cloudcomputing*-diensten, is dan ook begrijpelijk. De Raad onderschrijft de MvT voor wat betreft de voorgestelde reikwijdte van de bevoegdheid. Ook bij het voorbereiden en plegen van meer traditionele misdrijven zal het gebruik van moderne ICT-voorzieningen een steeds belangrijker component worden. Ook onderschrijft de Raad de expliciete uitsplitsing in het voorgestelde wetsartikel naar een aantal verschillende doelen waartoe in een geautomatiseerd werk kan worden binnengedrongen, omdat hiermee wordt bewerkstelligd dat reeds bij het vragen van de machtiging aan de rechter-commissaris concreet en helder wordt gemotiveerd waarvoor deze ingrijpende bevoegdheid zal worden toegepast.

Dit element van het Wetsvoorstel geeft de Raad verder aanleiding tot de volgende opmerkingen:

- Uit de MvT (p. 13 en 76) volgt dat de plaatsing van deze bevoegdheid in de zevende afdeling van Titel IV van het Wetboek van Strafvordering (enige bijzondere dwangmiddelen) impliceert dat onder andere de beperkte kennisneming van gegevens die betrekking hebben op verschoningsgerechtigden (art. 125l Sv) ook van toepassing is op het onderzoek in een geautomatiseerd werk. De Raad is van mening dat dit punt nadere toelichting zo niet regeling verdient. Zo is het de vraag op welke wijze communicatie met een verschoningsgerechtigde (bijvoorbeeld een advocaat) zal kunnen worden ontdekt en tijdig worden vernietigd conform artikel 126aa Sv. Uit de vereiste aanpassing van het Besluit technische hulpmiddelen strafvordering zal moeten blijken wat de functionaliteiten zijn van de software die de politie wil gaan inzetten. Ook zal daaruit moeten volgen of in die software een functie is ingebouwd die voorziet in de vernietiging van het resultaat van het aftappen van de communicatie met verschoningsgerechtigden. De Raad beveelt aan ook de wijziging van het Besluit te zijner tijd voor advies aan de Raad toe te laten zenden.
- Het spreekt voor zich dat bij het toepassen van deze bevoegdheid veelal ook de vraag naar de rechtsmacht aan de orde zal komen gelet op het niet aan landsgrenzen gebonden karakter van computercriminaliteit. Zoals in de MvT terecht wordt opgemerkt ziet artikel 32 van het Cybercrimeverdrag op de toegang, door middel van een netwerkzoeking, tot *opgeslagen gegevens* op het grondgebied van een andere verdragspartij en houdt dit artikel dus niet in het

binnendringen in een geautomatiseerd werk dat zich in het buitenland bevindt om *stromende gegevens* te verkrijgen. De Raad is van mening dat hieruit volgt dat de voorgestelde bevoegdheid ex artikel 125ja Sv niet kan worden ingezet met het oog op tapbevoegdheden. Het ware aan te bevelen deze grens uitdrukkelijk in de wet op te nemen en hierop in de MvT nader in te gaan.

Bevel tot ontoegankelijk maken van gegevens
De Raad heeft eerder geadviseerd over een conceptwetsvoorstel waarin was voorzien in aanpassing van de regeling van het ontoegankelijk maken van gegevens.[7] De Raad is verheugd dat een aantal in het eerdere advies gemaakte opmerkingen in het Wetsvoorstel en de MvT zijn terug te zien, zoals het vereiste van een machtiging van de rechter-commissaris (overeenkomstig de huidige regeling van art. 54a Sr). Enkele eerder gemaakte opmerkingen komen echter niet terug in het Wetsvoorstel en de MvT. De Raad adviseert deze hiermee aan te vullen. Het betreft:

- De vraag hoe om te gaan met de situatie waarin de aanbieder van de communicatiedienst niet in Nederland is gevestigd en waarin het strafbare feit niet in Nederland wordt begaan.
- Uitdrukkelijk te voorzien in een schadevergoedingsprocedure in het geval het beklag door de raadkamer van de rechtbank gegrond wordt verklaard of indien de strafrechter in zijn uitspraak alsnog besluit tot gehele of gedeeltelijke opheffing van de maatregel.
- De suggestie om in de wet tot uitdrukking te brengen dat het in dit verband – ten minste – moet gaan om een verdenking op het niveau van 'ernstige bezwaren'.

Het decryptiebevel aan de verdachte en artikel 6 EVRM
Volgens de MvT (p. 48) wordt de opsporing van computercriminaliteit belemmerd doordat gebruik wordt gemaakt van encryptie. Door gegevens te versleutelen kan worden voorkomen dat derden, die niet beschikken over een elektronische sleutel, kennis nemen van de inhoud van de gegevens. Het Wetsvoorstel voorziet daarom in de mogelijkheid dat de officier van justitie aan de verdachte het bevel richt toegang te verschaffen tot een geautomatiseerd werk of delen daarvan, tot een gegevensdrager of tot versleutelde gegevens.

Zoals in de MvT tot uitdrukking komt, is hier het in artikel 6 EVRM vervatte beginsel van nemo-tenetur in het geding (dit beginsel houdt in dat een persoon niet kan worden gedwongen mee te werken aan zijn eigen veroordeling). In de MvT (p. 56-60) wordt uitgebreid ingegaan op de verhouding tussen het voorgestelde bevel aan verdachte en de rechtspraak van het EHRM ten aanzien van artikel 6 EVRM. De conclusie hiervan is dat de voorgestelde regeling voor het decryptiebevel naar uw mening de toets van artikel 6 EVRM kan doorstaan. De Raad is er op voorhand niet van overtuigd dat dit het geval is. Voorts wil de Raad u erop wijzen dat een rechter in een concreet geval tot een andere conclusie kan komen, wat mogelijk consequenties heeft voor de bruikbaarheid van het bewijs van de resultaten van een dergelijk bevel. De Raad beveelt aan om de verhouding tussen het decryptiebevel en artikel 6 EVRM in de MvT

---

[7] Advies van de Raad van 30 september 2010, gepubliceerd op www.rechtspraak.nl onder nr. 2010/38.

nader te beschouwen en daarbij te betrekken de uitspraak van het EHRM in de zaak Chambaz[8] alsmede de daarop gevolgde discussie, waaronder de conclusie van A-G Wattel.[9]

Werklastgevolgen
Het Wetsvoorstel zal voor de Rechtspraak leiden tot enige werklastgevolgen, met name voor de rechter-commissaris. Per saldo zullen naar verwachting meer machtigingen inzake de inzet van bepaalde opsporingsbevoegdheden worden gevorderd. Het beoordelen van met name vorderingen tot machtigingen als bedoeld in de artikelen 125ja lid 4 Sv (binnendringen in geautomatiseerd werk) en 125k lid 6 Sv (decryptiebevel) op rechtmatigheid, proportionaliteit en subsidiariteit zal voor de rechter-commissaris een aanzienlijke inspanning vergen.[10] Ook voor de zittingsrechter zal het Wetsvoorstel werklastgevolgen hebben. In het verlengde van nieuwe strafbepalingen zullen zittingsrechters met nieuwe zaken te maken krijgen en daarover hebben te beslissen. Daarnaast is denkbaar dat door rechters-commissarissen afgegeven machtigingen ter toetsing aan zittingsrechters worden voorgelegd.

In welke mate van de ruimere bevoegdheden gebruik zal worden gemaakt, is op voorhand niet te kwantificeren. Vooralsnog gaat de Raad uit van een relatief klein aantal (ten opzichte van het totaal aantal strafzaken) als gevolg waarvan de werklastgevolgen naar verwachting niet van substantiële aard zullen zijn. De Raad behoudt zich het recht voor om hier op terug te komen indien na inwerkingtreding van het Wetsvoorstel in de praktijk blijkt dat het om grotere aantallen gaat.

Slot
Indien na het uitbrengen van dit advies het Wetsvoorstel op belangrijke onderdelen wordt gewijzigd of indien uit nadere uitvoeringsregelgeving belangrijke werklastgevolgen voortvloeien, dan wordt de Raad graag in de gelegenheid gesteld daarover aanvullend te adviseren. Met het oog op de voorbereiding van de gerechten op de invoering van het uiteindelijke Wetsvoorstel, stelt de Raad het op prijs als hij geïnformeerd wordt over de indiening van het Wetsvoorstel bij de Eerste Kamer en de plaatsing van de definitieve wetstekst in het Staatsblad.

Hoogachtend,

Waarnemend Voorzitter

[8] EHRM 5 april 2012, nr. 11663/04 Chambaz vs. Zwitserland). LJN BW5997, EHRC 2012/135.
[9] Conclusie van 1 maart 2013, LJN BZ3640.
[10] De werkbelasting van de rechter-commissaris per vordering ex artt. 125ja. 125k en 125p Sv wordt geschat op gemiddeld vijftien minuten (enigszins vergelijkbaar met het beoordelen van een vordering inzake een telefoon- of internettap).

Bijlage: opmerkingen van juridisch-technische aard

- Definitiebepaling artikel 80 sexies Sr

  Met het Wetsvoorstel wordt voorgesteld de definitiebepaling van een geautomatiseerd werk in artikel 80sexies Sr te verruimen, zodat ook het hacken van een router hieronder komt te vallen. Uit de MvT lijkt te volgen dat dit op dit moment op grond van wet en jurisprudentie niet strafbaar zou zijn.

  Het huidige artikel spreekt over *"een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen"*. In de MvT wordt gesteld dat de cumulatie van voornoemde drie voorwaarden problemen oplevert in het licht van de ontwikkeling van de informatie- en communicatietechnologie. Zo zou uit de jurisprudentie volgen dat het hacken van een router op dit moment niet strafbaar is als computervredebreuk (art. 138ab Sr), waarbij wordt verwezen naar een arrest van de Hoge Raad van 26 maart 2013.[11]

  Het is naar mening van de Raad de vraag of de in de MvT weergegeven interpretatie van dit arrest juist is. De Hoge Raad overweegt hierin immers als volgt:

  "Uit de zo-even weergegeven wetsgeschiedenis volgt dat een inrichting alleen als geautomatiseerd werk in de zin van de hier besproken wettelijke bepalingen kan worden aangemerkt indien zij geschikt is om drie functies te vervullen, te weten opslag, verwerking en overdracht van gegevens. Uit die wetsgeschiedenis volgt evenwel ook dat het begrip geautomatiseerd werk niet beperkt is tot apparaten die zelfstandig aan deze drievoudige eis voldoen. Ook netwerken bestaande uit computers en/of telecommunicatievoorzieningen heeft de wetgever onder het begrip 'geautomatiseerd werk' willen brengen, terwijl art. 138a (oud) Sr ook toepasselijk is op delen van zulke geautomatiseerde werken."

  Onder het huidige begrip 'geautomatiseerd werk' dient blijkens deze uitspraak (ook) te worden verstaan: netwerken bestaande uit computers en/of telecommunicatievoorzieningen. Aangezien een router deel uitmaakt van een dergelijk netwerk en artikel 138ab Sr ook toepasselijk is op delen van geautomatiseerde werken, komt het de Raad voor dat het hacken van een router reeds naar het huidige recht strafbaar is als computervredebreuk. De Raad stelt evenwel vast dat de voorgestelde wettekst hierover elke twijfel wegneemt, waartegen bij de Raad geen bezwaar bestaat.

- De Raad geeft in overweging de definitiebepalingen uit de artikelen 80septies en 80sexies Sr – overeenkomstig het eerdere conceptwetsvoorstel uit 2010 (artikelen 138e en 138f Sv) – op te nemen in het Wetboek van Strafvordering.

---

[11] HR 26 maart 2013, LJN BY9718.

- Bij het voorgestelde artikel 54a Sr: de Raad vraagt zich af of de huidige opzet van artikel 54a Sr niet beter is nu daaraan niet de (extra) voorwaarde van 'een strafbaar feit' wordt gesteld.

- In het voorgestelde artikel 125p Sv wordt verwezen naar de uitleg van het begrip 'ontoegankelijk maken' in artikel 125o, tweede lid, Sv. Daarbij wordt alleen de eerste volzin van dat lid van overeenkomstige toepassing verklaard. De Raad vraagt zich af waarom niet ook de tweede volzin daarvoor in aanmerking komt.

- In de MvT, artikelsgewijze toelichting op artikel I onderdeel D, wordt opgemerkt dat de maximale gevangenisstraf, die is voorzien in artikel 139e Sr, zal worden verhoogd van zes maanden naar een jaar. In het wetsontwerp wordt echter (nog) uitgegaan van een maximum van zes maanden gevangenisstraf.